

AMENDMENTS TO THE SPECIFICATION

(1) Please amend the paragraph on page 3, beginning on line 13, to read:

In the remainder of the present description and claims we shall define as SIM a SIM card typically involved in a GSM network or a USIM card ~~typically~~ typically involved in a UMTS network, or a similar card used in a different wireless network and provided with encryption based authentication or identification features, e.g., based on a challenge and response mechanism.

(2) Please amend the paragraph on page 12, beginning on line 16, to read:

It will be ~~appreciate~~ appreciated that the use of the cryptographic checksum MAC_K provides protection against unauthorized modifications of the encrypted sensitive data in terms of detection. In fact, an adversary, without the knowledge of the encryption key K , is not able to change the encrypted sensitive data along with the integrity of the cryptographic checksum MAC_K .

(3) Please amend the paragraph on page 14, beginning on line 14, to read:

In a step 210, these two session keys $Kc1$, $Kc2$ are subsequently mixed by means of ~~[[an]]~~ a hash function h , such as, but not limited to a SHA-1 function or a MD5 function.